Merton Mencap

Data Protection Policy

Last reviewed

February 2026

Next review

February 2028

This policy and procedure has been adopted by Merton Mencap through its Executive Committee which remains responsible for its review

Merton Mencap
Data Protection Policy

Aims of policy

This policy explains how Merton Mencap manages personal information. It explains the rights of people we hold information about and our responsibilities for obtaining, handling, processing, storing and destroying personal information.

The policy aims are to

- safeguard the people about whom we hold information by ensuring it is managed appropriately

- ensure Merton Mencap complies with its legal obligations under the Data Protection Act 2018 and General Data Protection Regulations (GDPR)

Introduction

The General Data Protection Regulation (GDPR) applies to organisations holding and using personal information which is held in electronic or manual filing systems, or which is obtained with the intention of being held in such systems.

An organisation which collects and uses personal information (or 'personal data') is called a Data Controller. The person to whom the personal data relates is called a Data Subject.

GDPR is based on the rights of the Data Subject to know which data being held about them by the Data Controller and how that data will be used. The regulation sets out principles so personal data is:

- obtained only for specified purposes
- processed fairly and lawfully
- relevant to the purposes for which it is processed
- accurate and kept up to date
- not kept for longer than necessary
- processed according to the rights of the Data Subject under the regulation
- protected against unauthorised processing, accidental loss or damage
- not transferred to areas outside of the European Union (including via websites)

Merton Mencap is responsible for determining the purpose and means of processing personal data.

The policy should be read alongside our other relevant documents including our Privacy Notices which can be found at www.mertonmencap.org.uk

Scope of policy

This policy applies to individuals for whom personal data is processed by Merton Mencap including employees, volunteers (including trustees), service users, members and supporters (eg donors).

It applies to people who *currently* have a relationship with Merton Mencap and those who *previously* had a relationship with us such as ex-employees or previous service users. We regard all individuals that fall into one of these categories as being Data Subjects for the purposes of this policy.

This policy covers the collection, maintenance, use and destruction of personal data, processes for sharing information and an individual's access to information.

Data protection principles

Merton Mencap recognises that personal data must be processed in accordance with 7 GDPR principles:

- processed lawfully, fairly and transparently
- collected and processed only for specified, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- be accurate and kept up to date
- not be kept for longer than is necessary for the purposes for which it is processed
- be processed with integrity and confidentiality
- that the organisation is accountable.

How we define personal data

Personal data means information which relates to an identifiable living person, the Data Subject, who can be identified from that data on its own or when put with other information which is likely to come into our possession. It includes an expression of opinion about them and an indication of the intentions of the organisation or others in respect of that person. It does not include anonymised data.

Personal data may be provided to us by the Data Subject or by someone else. For example, during the recruitment process, personal data may be provided by the Data Subject's former employer in the form of a reference. Personal data could also be created by us, for example if we raise an incident form to record a situation involving the Data Subject.

The types of personal data we collect and use about individuals is included in our relevant Privacy Notices.

Special categories of personal data

Special categories of personal data are types of personal data comprising information about an individual's

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- health
- sex life and sexual orientation
- criminal convictions and offences.

We may hold and use any of these special categories of personal data as detailed in our Privacy Notices.

How we define processing

Processing means any operation which is performed on personal data such as:

- collection, recording, organising, structuring or storing
- adapting or altering
- retrieving, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination, and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How we process personal data

We will process personal data (including special categories of personal data) to

- perform a contract, and/or
- comply with legal obligations, and/or
- pursue legitimate interests of our own or those of third parties (provided the applicant's interests and fundamental rights do not override those interests.)

We can process personal data for these purposes without the knowledge or consent of the individual. We will not use personal data for an unrelated purpose without telling the Data Subject about it and the legal basis that we intend to rely on for processing it.

Examples of when we might process an individual's personal data can be found in the relevant Privacy Notice. We will only process special categories of personal data in certain situations in accordance with the law.

We do not require individual consent to process special categories of personal data when we are processing it for the following purposes, which we may do:

- where necessary for carrying out rights and obligations under employment law
- where necessary to protect an individual's vital interests or those of another person, where either are physically or legally incapable of giving consent
- where an individual has made the data public
- where necessary for the establishment, exercise or defence of legal claims
- where necessary for the purposes of occupational medicine or for the assessment of working capacity
- where necessary to deliver appropriate services which meet individual needs
- where necessary in relation to working with children or vulnerable adults, e.g. criminal convictions, information identified via the Disclosure and Barring Service.

We may process special categories of personal data for the purposes stated in our Privacy Notices, in particular, we may use information to

- monitor equal opportunities
- monitor absence, assess fitness for work, to pay benefits, or to comply with our legal obligations under employment law including to make reasonable adjustments and to look after a person's health and safety

We do not take automated decisions about any individual using their personal data or use profiling in relation to any individual.

Sharing personal data

We may share personal data with other organisations to carry out our obligations under our contract with an individual or for legitimate interests.

We require those organisations we share data with to protect it in accordance with the law, and to only process data for the lawful purpose for which it has been shared and in accordance with our instructions.

A condition of our sharing personal data with third parties is their confirmation of their normal (regular) data processing activities all occurring within the European Union/ European Economic Area, with all databases, servers, and backups located in EU/EEA data centres.

They have also confirmed that data will not be transferred outside this area, unless the third country has been deemed by the EU Commission to ensure an appropriate level of protection, the recipient of the data guarantees an acceptable level of data protection in accordance with EU standard contractual clauses for the transmission of personal data, or there are other safeguards in place that permit such a transfer.

See appendix 1 for details of organisations with whom we share personal data.

Responsibilities

The Executive Committee of Merton Mencap is responsible for this policy, its review and for ensuring it is being implemented.

The Chief Executive of Merton Mencap is the organisation's Data Protection Officer (DPO) responsible for ensuring employees and volunteers are aware of and act on their responsibilities.

The DPO can be contacted:

Email: chief.executive@mertonmencap.org.uk
Phone: 07767 670 134

The DPO details are stated:

- on the charity's web site (Contact Us page)
- in this Policy which is published on our web site
- in the staff Handbook

All employees and volunteers at Merton Mencap have responsibility for ensuring personal data is collected, stored and handled in line with this policy.

Employees and volunteers must only access personal data if they need it for the work they do for or on behalf of Merton Mencap, and must only use it for the purpose for which it was obtained. Any doubts regarding accessing or using personal data should be addressed to their line manager or the Data Protection Officer.

In any case, all staff and volunteers are required to adhere to these instructions:

General

- Be vigilant at all times about keeping personal data safe and secure
- Only share personal data with others within Merton Mencap who need it as part of their work with the organisation
- Do not share personal data with people outside the organisation without first checking with a line manager or Data Protection Officer
- Regularly review and update personal data which you have as part of your role. This includes advising Merton Mencap if your own personal data changes
- Do not make unnecessary copies of personal data
- Do not remove personal data from Merton Mencap premises without authorisation from a line manager. Personal data must be returned after use.
- Avoid taking personal data into the community (eg for meetings or for a community activity) and anonymise data wherever possible
- Avoid people outside of the organisation overhearing when having discussions which refer to personal data

- Dispose of personal data securely, eg never place documents containing personal data in general waste bins, always dispose of securely (destroy in our shredders or dispose via our confidential waste provider)
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Chief Executive.

Electronic devices (eg computers, tablets, mobile phones)

- Ensure passwords contain at least 8 characters of lowercase and uppercase letters, numbers, and symbols (see appendix 2, Better Password Security)
- Update passwords at least annually and inform the Office Manager of password updates
- Always lock devices when not in use
- Do not save personal data to personal devices unless first authorised by a line manager
- Do not use any portable storage devices (eg USB sticks)
- Do not share personal data during online meetings (eg avoid referring to service users by name during Zoom/Teams meetings)
- Where possible, anonymise personal data when communicating by email. If it is not possible to anonymise personal data over email, use our confidential electronic transfer system when emailing personal date to recipients without a Merton Mencap email address

Office

- Keep desks clear of personal information when not attending/after use
- Lock drawers and filing cabinets when not attending/after use
- Avoid discussions involving personal data from being overheard by people outside of our organisation and by colleagues who do not need to know information as part of their job at Merton Mencap.

Data retention

Our normal data retention periods are as follows:

Employee and volunteer records:

- HR files to be kept for 6 years following person leaving
- After 6 years, we will keep a record of the staff name, date of birth, job title, salary, and start and finish dates for the purpose of responding to reference requests and managing the charity's Pension
- We will keep health and sickness records, accident and incident reports and any health and safety records for a period of 40 years
- We will keep parental leave records for 18 years

Records in relation to adult service users (ie adults with a learning disability and/or autism and their carers:

- All records will normally be kept for 8 years from the date of ceasing to use our services

- After 8 years, we will keep a record of the service user's name and date of birth for identification, plus start and end dates of service use
- We will keep records of non-serious incidents involving the service users for 10 years from the date of the incident
- We will keep records of any serious incidents for 20 years from the date of the incident.

Records in relation to child/young person service users (ie children/young people with a learning disability and/or autism and their parents:

- All records will normally be kept until their 25th birthday (26th birthday if they are still accessing a service from us at the age of 17).
- After their 25th or 26th birthday, we will keep a record of the service user's name and date of birth for identification, plus start and end dates of service use.
- We will keep records of non-serious incidents for 10 years from the date of the incident.
- We will keep records any serious incidents for 20 years from the date of the incident.

These are normal intended retention periods. Individuals can still exercise their right to request that personal data is erased before the retention period ends (see rights of data subjects below).

When retention periods end, we will destroy hard copy documents through an appropriate confidential waste disposal provider and delete from our systems data held electronically.

The rights of data subjects

All individuals have the right to information about the personal data we process, how and on what basis as set out in this policy. Individuals can exercise these rights by contacting the Data Protection Officer.

Individuals have the right to

- access their own personal data by way of a Subject Access Request (see below)
- request that we correct any inaccuracies in their personal data
- request that we erase personal data where we are not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected
- apply for the use of personal data to restricted, including while a request to correct or erase personal data is being considered
- object to data processing where we are relying on a legitimate interest to do so if it is considered that their rights and interests outweigh our own
- object if we process their personal data for the purposes of our communications even if consent has been previously given
- receive a copy of their personal data and to transfer personal data to another data controller. Merton Mencap will not charge for this and will in most cases aim to do this within one month

- not be subjected to automated decision-making.
- be notified of a data security breach concerning your personal data.

In most situations we will not rely on an individual's consent as a lawful ground to process personal data. If we do however request consent to the processing of personal data for a specific purpose, an individual has the right not to consent or to withdraw consent later.

Individuals have the right to complain to the Information Commissioner, by contacting the Information Commissioner's Office directly, the details of which can be found at www.ico.org.uk.

Subject Access request

Data subjects can make a Subject Access Request (SAR) to find out the information Merton Mencap's holds about them.

The procedure for managing a SAR can be found at appendix 3.

How to deal with data breaches

Merton Mencap has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of any personal data occur it must be reported and we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the CEO immediately and keep any evidence you have in relation to the breach.

Merton Mencap
Data Protection Policy

Appendix 1: Organisations with whom we share personal data

Relating to all individuals:

- **Microsoft**: cloud-based storage of documents and email
- **X, Instagam, Facebook, YouTube**: social media posts
- **WSM**: auditors
- **Lamplight Database Systems Ltd**: central database and case management
- **Sage (UK) Ltd:** accounting software and support
- **Qlic IT Ltd**: IT support services
- **Daisy Communications Ltd**: mobile phone services
- **CFH Docmail Ltd**: postal services
- **Vision Mission Ltd**: fundraising support services
- **Merton council & NHS:** reporting for statutory service delivery; payroll services
- **Grenke leasing Ltd:** photocopier & printing
- **Mailchimp:** ebulletin distribution
- **EventBrite:** event bookings
- **Firetext:** text messaging facility
- **WhatsApp:** text messaging and call facility
- **Adam Bradford Ltd:** web site updates
- **The Grange:** hire for registered office
- **Sum Up:** credit card payment facility
- **AJG Gallagher:** insurances
- **Rose Hill cars:** taxi services
- **Thames Valley Adventure Playground:** activity provider

Relating to employees & volunteers:

- **The HR Consultancy Ltd**: human resources services
- **Hospital Saturday Fund**: health plan services
- **Acorn Occupational Health Ltd**: occupational health services
- **DataPlan**: payroll services
- **The Pension Trust**: pension services
- **HMRC**: tax records
- **Information Commissioners Office (ICO)**: data related matters
- **Natwest Bank**: bank (payroll)
- **Handelsbanken, CCLA**: bank
- **Caxton**: top-up cards
- **PayPal**: donation facility
- **iHasco, TutorCare, Direct OT, Caring for Care, St John's Ambulance, Socail care TV**: training
- **Protocol & Sugarman Education**: staff agency
- **CharityJob**: recruitment agency

Relating to service users:

- **Ofsted**: Office for standards in education, children's services and skills

Merton Mencap
Data Protection Policy

Appendix 2: Better password security

- Create a secure password that makes sense to you but not to others.
- Don't tell anyone your password (unless someone authorised at Merton Mencap needs it)
- Be sure no one watches when you enter your password
- Always log off if you leave your device, even if you're away for a short time
- Avoid consecutive keyboard combinations such as qwerty, asdfg, 123345, and slang terms, common misspellings and words spelt backwards
- Avoid simple passwords such as first names of partners, family members, relatives and pets all of which may be found with research as the answers may be on the person's social media profile
- Avoid reusing passwords for multiple accounts which can lead to identity theft.
- Avoid entering passwords on to devices you don't control (eg computers at internet cafés or libraries). Malware may steal your passwords.
- Avoid entering passwords when using unsecured Wi-Fi connections as hackers can intercept passwords and data over this unsecured connection.
- Strong passwords are easy to remember but hard to guess, for example, Iam:)2b29! has10 characters and says "I am happy to be 29!".
- Ensure reminders for passwords are always stored securely, away from your devices and mixed with other numbers and letters so it's not apparent that it's a password

Merton Mencap
Data Protection Policy

Appendix 3: Subject Access Request Procedure

Roles & responsibilities

Data Protection Officer (DPO)	Responsible for ensuring the SAR is responded to as per this policy and procedure
Employees	Responsible for ensuring that a request for data by any party is forwarded to the DPO immediately by email

Terms

Data Subject	The identified or identifiable living individual to whom personal data relates.
Personal Data	Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question, or who can be indirectly identified from that information in combination with other information.
Subject Access Request	A formal inquiry made to a company by a data subject inquiring what of the data subject's personal information has been collected, stored, and used (processed).

Procedure

Logging a request
Once a SAR has been received by the DPO, they will log the date and advise the Chair of Trustees of the timescale for response, referring to ICO and government guidance.

Valid SAR
A valid SAR can be received in any format in writing or verbally. An individual does not need to use specific wording to define their request for a SAR.

The DPO will take reasonable measures to identity the individual making the request is authentic, e.g. by contacting them in a way other than the method of request.

Once the request has been validated, the DPO will confirm to the individual the timescale for response and the secure method to which information will be provided.

Locating information for the SAR
The DPO will work with relevant Merton Mencap staff to identify systems where data is being held and to carry out searches to identify personal data on the individual (Data Subject), so it can be reviewed before providing it.

Reviewing personal information & what can be disclosed as a result of a SAR
Once information has been collated on the Data Subject, the DPO will review what can be disclosed, which is done on a case-by-case basis.

For example, parts of a document may need to redacted to avoid reference to another individual. If needed, third parties may be contacted for consent to disclose their information in the SAR.

The DPO will consider whether any exemptions apply before releasing information to the Data Subject.

Providing information to the Data Subject
When the DPO has identified all the information that can be sent in response to a SAR, they will conduct one final review of this information as a collection of data.

Personal data of the Data Subject will be provided in the secure means agreed by the date given.
